

REMARKS/ARGUMENTS

This paper is in response to the non-final Office Action of November 7, 2005. Applicants amended independent claims 1, 10, and 16 and dependent claims 13, 17, and 18. Claims 8 and 11 have been canceled. Claims 21 and 22 have been added. The amended and added claims introduce no new matter and are fully supported by the specification. Accordingly, Applicants respectfully request examination of pending claims 1-7, 9-10, and 12-22.

Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 10 and 12 under 35 U.S.C. § 102(b) as being anticipated by Veil et al. (US Patent No. 6,092,202). This rejection is traversed in light of the amendments and arguments contained herein.

In contrast with the recited features of independent claim 10 as amended herein, Veil et al. fails to teach or suggest an encryption engine including a “plurality of encryption/decryption channels” and a “control logic that is configured to determine which encryption/decryption channel is available and direct encrypted data passing through the hub to available encryption/decryption channels.” Specifically, Veil et al. is completely silent as to the “security co-processor” having a data communications flow management component (i.e., control logic) that manages data communications from a plurality of communications channels to and from the “security co-processor.” Furthermore, Veil et al. teaches that “the security co-processor is responsible for retrieving the sensitive data from the smart cards” (See Veil et al., column 7, lines 33-36) which indicates that there is no middle-layer component (i.e., control logic) configured to manage data communications flow

between multiple channels of communication leading to and from the “security co-processor.”

Additionally, Veil et al. fails to disclose or teach “a system tray program configured to allow customization of hub features.” Specifically, the Applicants submit that Veil et al. is silent as to the functionality or features of the “security co-processor” being customizable.

Further, in contrast with amended claim 10, Veil et al. does not disclose a “portable encryption control device.” Specifically, the “security co-processor” disclosed in Veil et al. requires “a host interface for interfacing with a host computer” (See Veil et al., Column 7, lines 1-5). There is no disclosure whatsoever in Veil et al. that indicates that the “security co-process” can be a “portable” unit that can be readily attached and detached from a computer system without the use of a “host interface.”

For at least the above reasons, Applicants respectfully submit that Veil et al. fails to anticipate each and every feature of independent 10 as amended. Claims 12-15 depends directly from claim 10. Applicants respectfully request that this rejection be withdrawn for claims 10 and 12-15.

The Examiner rejected claims 1, 7 and 9 under 35 U.S.C. § 102(b) as being anticipated by Vu et al. (US Patent No. 6,557,104). This rejection is traversed in light of the amendments and arguments contained herein.

In contrast with the recited features of independent claim 10 as amended herein, Vu et al. fails to teach or suggest a hub containing a “hub microprocessor and an encryption engine configured to encrypt/decrypt data communications...” Specifically, Vu et al. teaches that their “token may include any type of removable physical storage device, such as a magnetic strip, PCMCIA card, floppy disk CD-

ROM or any other similar removable storage device” and that “the token does not need to contain its own processor and accompanying hardware, since the PROCESSING WILL TAKE PLACE IN THE MAIN SYSTEM PROCESSOR” (See Vu et al., column 4, lines 21-36; and Figure 5). As such, the “token reader” (i.e., hub) taught by Vu et al. can be any “dumb” removable storage device reader such as a tape reader and CD-ROM drive which do not have or require separate microprocessors or encryption engines as the encryption/decryption processing takes place entirely in the “main system processor” (i.e., the computer system) that the “token reader” is attached to (See Vu et al., Figure 5).

Claim 1, as amended herein, further includes the features of “an installed system tray program configured to allow customization of hub features” and an “encryption engine including, a plurality of encryption/decryption channels and a control logic... configured to determine which encryption/decryption channel is available and direct encrypted data passing through the hub to available encryption/decryption channels.” Vu et al. is completely silent as to those features.

For at least the above reasons, Applicants respectfully submit that Vu et al. fails to anticipate each and every feature of independent 1 as amended. Claims 2-7 and 9 depends directly from claim 1. Applicants respectfully request that this rejection be withdrawn for claims 1-7 and 9.

Rejections under 35 U.S.C. § 103(a)

Claims 5, 6 and 16-19 were rejected as being unpatentable over Vu et al. in view of Veil et al. In light of the amendments and arguments contained herein, Applicants respectfully request reconsideration of this rejection.

As a preliminary matter, claims 5 and 6 depend off of independent claim 1, which for the reasons elaborated above should be allowed. Veil et al. fails to cure the deficiencies of Vu et al., as it is silent as to the “hub” including “a system tray program configured to allow customization of hub features” and an encryption engine with a “plurality of encryption/decryption channels and a control logic.” Therefore, the Applicants respectfully request that this rejection be withdrawn for claims 5 and 6.

In contrast with the recited features of claim 16, as amended herein, Vu et al. fails to disclose an encryption control device (ECD) containing an “ECD microprocessor and an encryption engine configured to encrypt/decrypt data communications” for at least the reasons discussed above. Additionally, Vu et al. is silent as to the ECD unit having an “encryption engine including, a plurality of encryption/decryption channels and a control logic... configured to determine which encryption/decryption channel is available and direct encrypted data passing through the hub to available encryption/decryption channels.” For at least the same enumerated reasons discussed above, Veil et al. fails to cure the deficiencies in Vu et al. as it is also silent as to those features.

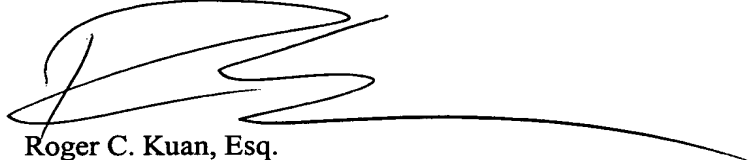
As such, for at least the above reasons, Applicants respectfully request that this rejection be withdrawn for independent claim 16 and claims 17-20 which depend directly or indirectly from it. Claims 21-22 are new and recite features that are not taught or disclosed by any of the references asserted by the Examiner. Therefore, Applicants respectfully submit that claims 21-22 are in condition for allowance.

SUMMARY

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner has any questions concerning the present Amendment, the Examiner is kindly requested to contact the undersigned at (408) 774-6927. If any additional fees are due in connection with filing this Amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. ADAPP201A). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP



Roger C. Kuan, Esq.
Reg. No. 56,558

MARTINE PENILLA & GENCARELLA, LLP
710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Tel: (408) 749-6900
Customer No. 25,920